LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-8. (Cancelled)

11-27. (Cancelled)

28. (Currently Amended) A method of automatically obtaining a second certificate for a user in a Public Key Infrastructure (PKI) enterprise using a first certificate, the method comprising:

accessing a registration server using a user's server and the first certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's first certificate;

creating a secure data channel between the registration server and the user server;

forwarding a request for the second certificate from the user server to the registration server;

determining in the registration server that the user is entitled to the second certificate by ensuring that the user is still a member of the PKI enterprise and ensuring that the user does not already have the second certificate;

forwarding a request from the registration server to an authority to generate a private/public key pair;

sending the private key to the user from the authority via the secure data channel;

sending the public key from the authority to another authority to be signed; and

forwarding the second certificate from the another authority to a directory.

29. (Previously Presented) The method of claim 28, further comprising sending a backup copy of the private key from the authority to a key recovery authority.

30. (Previously Presented) The method of claim 28, wherein the first certificate comprises a signature certificate.

31. (Previously Presented) The method of claim 28, wherein the second certificate comprises an encryption certificate.

32. (Previously Presented) The method of claim 28, wherein the first certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate.

33. (Previously Presented) The method of claim 28, wherein the first certificate comprises a signature certificate and the second certificate comprises a replacement encryption certificate.

34. (Previously Presented) The method of claim 28, wherein the first certificate comprises a signature certificate and the second certificate comprises one of either the user's current encryption certificate or an expired encryption certificate of the user.

35. (Currently Amended) A method of automatically obtaining a second certificate for a user in a Public Key Infrastructure (PKI) enterprise using a first certificate, the method comprising:

accessing a server platform using a user's server and the first certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's first certificate;

tracking a pedigree of the user's first certificate;

accessing a registration web page having a level of security that is commensurate with the pedigree of the user's first certificate;

creating a secure data channel between the server platform and the user server;

forwarding a request for the second certificate from the user server to the server platform; and

generating at the server platform the second certificate.

36. (Previously Presented) The method of claim 35, wherein the first certificate comprises a signature certificate.

37. (Previously Presented) The method of claim 35, wherein the second certificate comprises an encryption certificate.

38. (Previously Presented) The method of claim 35, wherein the first certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate.

39. (Previously Presented) The method of claim 35, wherein the first certificate comprises a signature certificate and the second certificate comprises a replacement encryption certificate.

40. (Previously Presented) The method of claim 35, wherein the first certificate comprises a signature certificate and the second certificate comprises one of either the user's current encryption certificate or an expired encryption certificate of the user.

41. (Currently Amended) An apparatus for automatically obtaining a ~~second~~ replacement certificate for a user in a Public Key Infrastructure (PKI) enterprise using a ~~first~~ signature certificate, the apparatus comprising:

a user server and a registration server, the user server accessing the registration server using the ~~first~~ signature certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's ~~first~~ signature certificate;

a secure data channel, the secure data channel being disposed between the registration server and the user server, the user server forwarding a request for the ~~second~~ replacement certificate to the registration server through the secure data channel;

a first authority, the registration server determining that the user is entitled to the ~~second~~ replacement certificate and, upon said determination, revoking a certificate which the replacement certificate is replacing and forwarding a request to the first authority to generate a private/public key pair associated with the replacement certificate, the first authority sending the private key to the user via the secure data channel;

a second authority, the first authority sending the public key to the second authority to be signed; and

a directory, the second authority forwarding the ~~second~~ replacement certificate to the directory.

42-43. (Cancelled)

44. (Previously Presented) The apparatus of claim 41, wherein the first certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate.

45. (Currently Amended) The apparatus of claim 41, wherein ~~the first certificate comprises a signature certificate and~~ the second certificate comprises a replacement encryption certificate.

46. (Cancelled)

47. (Currently Amended) An apparatus for automatically obtaining a second certificate for a user in a Public Key Infrastructure (PKI) enterprise using a ~~first~~ signature certificate, the apparatus comprising:

a user server and a server platform, the user server accessing the server platform using the ~~first~~ signature certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's ~~first~~ signature certificate;

a secure data channel, the secure data channel being disposed between the server platform and the user server and being encrypted using the signature certificate;

the user server forwarding a request for the second certificate to the server platform; and

the server platform generating the second certificate.

48. (Cancelled)

49. (Previously Presented) The apparatus of claim 47, wherein the second certificate comprises an encryption certificate.

50. (Currently Amended) The apparatus of claim 47, wherein the ~~first~~ signature certificate comprises an expiring signature certificate and the second certificate comprises a replacement signature certificate.

51. (Currently Amended) The apparatus of claim 47, wherein ~~the first certificate comprises a signature certificate and~~ the second certificate comprises a replacement encryption certificate.

52. (Currently Amended) The apparatus of claim 47, wherein ~~the first certificate comprises a signature certificate and~~ the second certificate comprises one of either the user's current encryption certificate or an expired encryption certificate of the user.

53. (New) The method of claim 28, further comprising revoking the first certificate upon determining that the user is entitled to the second certificate.

54. (New) The method of claim 53, further comprising signaling both the directory and the another authority that the first certificate has been revoked.

55. (New) The method of claim 28, wherein accessing a registration server comprises tracking a pedigree of the user's first certificate to access a registration web page having a level of security that is commensurate with the pedigree of the user's first certificate.

56. (New) The method of claim 30, wherein the second certificate is an encryption certificate, and wherein creating a secure data channel comprises encrypting a transmission between registration server and the user server using the signature certificate.

57. (New) The method of claim 35, wherein the server platform is a key recovery authority, and wherein the second certificate is one of a current encryption certificate and an expired encryption certificate.

58. (New) The method of claim 35, further comprising determining in the server platform that the user is entitled to the second certificate by ensuring that the user is still a member of the PKI enterprise and ensuring that the user does not already have the second certificate.

59. (New) The method of claim 58, further comprising revoking the first certificate upon determining that the user is entitled to the second certificate.

60. (New) The method of claim 59, further comprising signaling both the directory and the another authority that the first certificate has been revoked.

61. (New) The method of claim 35, wherein the second certificate is an encryption certificate, and wherein creating a secure data channel comprises encrypting a transmission between registration server and the user server using the signature certificate.

62. (New) The apparatus of claim 41, wherein the registration server comprises a plurality of registration web pages, each of the plurality of registration web pages having a level of security, a given one of the plurality of registration web pages being accessible to a given user in the PKI enterprise upon a pedigree of the given user's signature certificate being commensurate with the respective level of security.

63. (New) The apparatus of claim 41, wherein the secure data channel is encrypted using the signature certificate.

64. (New) The apparatus of claim 47, wherein the server platform comprises a plurality of registration web pages, each of the plurality of registration web pages having a level of security, a given one of the plurality of registration web pages being accessible to a given user in the PKI enterprise upon a pedigree of the given user's signature certificate being commensurate with the respective level of security.

65. (New) The apparatus of claim 47, wherein the server platform determines whether the user is entitled to the second certificate by ensuring that the user is still a member of the PKI enterprise and by ensuring that the user does not already have the second certificate upon the user server forwarding the request for the second certificate.

66. (New) The apparatus of claim 47, wherein the server platform revokes the signature certificate upon the server platform generating the second certificate.

67. (New) The apparatus of claim 47, wherein the server platform is a key recovery authority, and wherein the second certificate is one of a current encryption certificate and an expired encryption certificate.